CLAIMS

What is claimed is:

1. A method of enabling or activating a protected function, said method comprising:

storing an authorization code in a wireless communication device;

transmitting an access request from said wireless communication device to an access control device;

receiving an authentication challenge from said access control device at said wireless communication device in response to said access request;

computing an authentication response based on said authentication challenge and said authorization code; and

transmitting said authentication response from said wireless communication device to said access control device.

2. The method of claim 1 wherein storing an authorization code in said wireless communication device comprises generating an authorization code based on a combination of a secret code and a time indication to limit access to said protected function to a defined time period.

3. The method of claim 1 wherein generating an authorization code based on a combination of a secret code and a time indication further comprises combining a device identifier associated with said access control device with said secret code and said time indication.

4. The method of claim 2 wherein storing an authorization code in said wireless communication device comprises storing a plurality of authorization codes in said wireless communication device, each said authorization code being associated with a different time period.

5. The method of claim 1 wherein storing an authorization code in said wireless communication device comprises storing said authorization code in a smart card associated with said wireless communication device.

6. The method of claim 1 wherein transmitting an access request from said wireless communication device to an access control device comprises transmitting a device identifier associated with said access control device to said access control device.

7. The method of claim 6 wherein transmitting a device identifier associated with said access control device to said access control device comprises transmitting a group identifier derived from said device identifier.

8. The method of claim 1 wherein computing an authentication response based on said authentication challenge and said authorization code comprises combining selected portions of said authentication challenge and said authorization code with a non-reversible function.

9. The method of claim 1 wherein said authentication challenge includes at least a random number and wherein computing an authentication response based on said authentication challenge and said authorization code comprises combining said random number of said authentication challenge and said authorization code.

10. The method of claim 9 wherein computing an authentication response based on said authentication challenge and said authorization code further comprises combining a device identifier associated with said access control device with said random number of said authentication challenge and said authorization code.

11. The method of claim 1 wherein protected function is unlocking a door.

12. The method of claim 1 further comprising transmitting electronic identity from said wireless communication device to a central controller and receiving said authorization code from said central controller following verification of said electronic identity.

13. The method of claim 12 wherein said electronic identity is a credit identity of a user verified by a credit agency.

14. The method of claim 12 wherein transmitting electronic identity from said wireless communication device to a central controller comprises transmitting said electronic identity to said central controller via a wireless communication interface.

15. A method of enabling or activating a protected function, said method comprising:

receiving an access request from a wireless communication device at an access control device;

transmitting an authentication challenge from said access control device to said wireless communication device in response to said access request;

receiving an authentication response based on said authentication challenge and an authorization code;

comparing said received authentication response with an expected authentication response; and

generating a control signal to permit access to said protected function if said received authentication response matches said expected authentication response.

16. The method of claim 15 further comprising storing said authorization code in said access control device.

17. The method of claim 16 wherein storing said authorization code in said access control device comprises storing a plurality of authorization codes in said access control device, each authorization code being valid for a defined time period.

18. The method of claim 15 further comprising computing said authorization code based on a combination of a secret code and a time indication.

19. The method of claim 18 wherein computing said authorization code based on a combination of a secret code and a time indication is performed by said access control device.

20. The method of claim 18 wherein computing said authorization code based on a combination of a secret code and a time indication is performed by a central controller in communication with said access control device.

21. The method of claim 18 wherein computing said authorization code based on a combination of a secret code and a time indication further comprises combining a device identifier associated with said access control device with said secret code and said time indication.

22. The method of claim 15 wherein said access request includes a device identifier to address said access control device, and wherein said method further comprises reading said device identifier and transmitting said authentication challenge only if a correct device identifier is received by said access control device.

23. The method of claim 15 further comprising computing said authentication challenge.

24. The method of claim 23 wherein computing said authentication challenge is performed by said access control device.

25. The method of claim 23 wherein computing said authentication challenge is performed by a central controller in communication with said access control device.

26. The method of claim 23 wherein computing said authentication challenge comprises generating a random number.

27. The method of claim 26 wherein computing said authentication challenge comprises combining said random number with a time indication.

28. The method of claim 15 further comprising computing said expected authentication response.

29. The method of claim 28 wherein computing said expected authentication response is performed by said access control device.

30. The method of claim 28 wherein computing said expected authentication response is performed by a central controller in communication with said access control device.

31. The method of claim 28 wherein computing said expected authentication response comprises combining selected portions of said authentication challenge and said authorization code.

32. The method of claim 31 wherein computing said expected authentication response further comprises combining a device identifier associated with said access control device with said selected portion of said authentication challenge and said authorization code.

33. The method of claim 31 wherein said authentication challenge includes at least a random number and where combining selected portions of said authentication challenge and said authorization code comprises combining said random number with said authorization code.

34. The method of claim 31 wherein combining selected portions of said authentication challenge and said authorization code comprises combining said selected portions of said authentication challenge and said authorization code using a non-reversible function.

35. The method of claim 15 wherein said protected function is unlocking a door.

36. A method of programming a wireless communication device with an authorization code used to enable or activate a protected function, said method comprising:

storing a master code in a central controller;

receiving an initialization request from said wireless communication device;

computing an authorization code based on said master code, said central controller in response to receipt of said initialization request;

communicating said authorization code to said wireless communication device.

37. The method of claim 36 further comprising storing said authorization code in said wireless communication device.

38. The method of claim 36 wherein storing a master code in a central controller comprises storing said master code in a tamper-resistant security module.

39. The method of claim 36 wherein said initialization request includes an electronic identity of the requesting party and wherein said method further comprises authenticating the electronic identity of the requesting party.

40. A device for enabling or activating a protected function, said device comprising:

memory to store an authorization code;

a wireless transmitter to transmit an access request and an authentication response to an access control device;

a wireless receiver to receive an authentication challenge from said access control device responsive to said access request;

a processor to compute said authentication response based on said authentication challenge received from said access control device and said authorization code.

41. The device of claim 40 wherein said authorization code is based on a master code.

42. The device of claim 41 wherein said authorization code comprises a combination of said master code and a time indication to limit access to said protected function to a defined time period.

43. The device of claim 42 wherein said memory stores a plurality of authorization codes for a plurality of defined time periods.

44. The device of claim 41 wherein said authorization code comprises a combination of said master code with identification code associated with said protected function.

45. The device of claim 44 wherein said identification code uniquely identifies said protected function.

46. The device of claim 45 wherein said identification code comprises a plurality of symbols and wherein a subset of said symbols identifies a group of access control devices.

47. The device of claim 40 wherein said protected function is the ability to unlock a door and wherein said authorization code unlocks said door.

48. The device of claim 40 wherein said wireless transmitter is a short-range wireless transmitter.

49. The device of claim 48 wherein said wireless receiver is a short-range wireless receiver.

50. The device of claim 49 wherein said wireless transmitter and said wireless receiver comprise a BLUETOOTH transmitter and BLUETOOTH receiver respectively.

51. The device of claim 40 further comprising a cellular radiotelephone transceiver for communicating with a mobile communication network.

52. The device of claim 40 further comprising a tamper-resistant security module containing said processor.

53. The device of claim 52 wherein said tamper resistant security module comprises a smart card.

54. The device of claim 40 wherein said processor combines selected portions of said authentication challenge with said authorization code to generate said authentication response.

55. The device of claim 54 wherein said processor further combines said selected portions of said authentication challenge and said authorization code with an identification code associated with said protected function to generate said authentication response.

56. The device of claim 54 wherein said selected portions of said authentication challenge includes at least a random number contained in said authentication challenge.

57. The device of claim 40 wherein said device exchanges messages with a central controller according to a predetermined protocol to obtain said authorization code.

58. The device of claim 57 wherein said device transmits its identity to said central controller as part of said predetermined protocol to enable its identity to be authenticated by said central controller.

59. The device of claim 58 wherein said identity is the credit identity of a user verified by a credit agency.

60. An access control device to secure a protected function, said access control device comprising:

a wireless transceiver to communicate with a wireless communication device;

a processor programmed to:

generate an authentication challenge in response to an access request from said wireless communication device;

transmit said authentication response via said wireless transceiver to said wireless communication device;

receive an authentication response from said wireless communication device via said wireless transceiver;

compare said received authentication response to an expected authentication response based on said authentication challenge and an authorization code; and

generate a control signal to permit access to said protected function if said expected authentication response matches said received authentication response.

61. The access control device of claim 60 further comprising memory to store a master code, said processor being further programmed to compute said authorization code based on said master code.

62. The access control device of claim 61 wherein said processor computes said authorization code by combining said master code with a time indication associated with a time period during which said authorization code is valid.

63. The access control device of claim 62 wherein said processor computes said authorization code by further combining a device identifier with said master code and said time indication.

64. The access control device of claim 62 further comprising a tamper resistant security module containing said memory.

65. The access control device of claim 60 wherein said authentication challenge comprises a random bit pattern.

66. The access control device of claim 64 further comprising a random bit generator to generate said random bit pattern.

67. The access control device of claim 65 wherein said authentication challenge generated by said processor further comprises a time indication.

68. The access control device of claim 60 further comprising an actuator responsive to said control signal to unlock a door.

69. The access control device of claim 60 wherein said access control device is identified by a device identifier and wherein said processor is programmed to respond to access requests containing at least a portion of said device identifier.

70. The access control device of claim 60 further comprising a clock to provide a time indication to said processor to use to validate an authentication response.

71. The access control device of claim 70 wherein said processor is responsive to a reset command to reset said clock to a time indicated in said reset command.

72. A device for issuing authorization code to activate or enable a protected function, said device comprising:

memory to store a master code;

an interface to communicate with a wireless communication device;

a processor programmed to:

compute an authorization code based on said master code in response to receipt of an initialization request from said wireless communication device;

transmit said authorization code to said wireless communication device.

73. The device of claim 72 further comprising a tamper resistant security module containing said memory to hinder extraction of said master code from said memory.

74. The device of claim 72 wherein said interface is a wireless interface.

75. The device of claim 74 wherein said interface is a wireless BLUETOOTH interface.

76. The device of claim 75 wherein said processor is programmed to execute an authentication procedure in response to receipt of said initialization request.

77. The device of claim 76 wherein said processor authenticates a claimed electronic identity received from said wireless communication device as part of said authentication procedure.